

# **PRIVACY IMPACT ASSESSMENT**

*Financial Management Systems*

**Risk Management Agency**

May 2003

# **PRIVACY IMPACT ASSESSMENT**

## **Financial Management Systems**

### **TABLE OF CONTENTS**

	<u>Page #</u>
<b>1.0    <i>PRIVACY IMPACT ASSESSMENT METHODOLOGY</i> .....</b>	<b>3</b>
<b>1.1    Background .....</b>	<b>3</b>
<b>1.2    Applicable laws, regulations, policies and procedures .....</b>	<b>3</b>
<b>1.3    Systems of Records Notice .....</b>	<b>3</b>
<b>2.0    <i>ROLES AND RESPONSIBILITIES</i>.....</b>	<b>4</b>
<b>3.0    <i>ASSESSMENT</i>.....</b>	<b>4</b>
<b>3.1    Data in the system.....</b>	<b>4</b>
<b>3.2    Access to the data.....</b>	<b>5</b>
<b>3.3    Attributes of the data .....</b>	<b>5</b>
<b>3.4    Maintenance of Administrative controls .....</b>	<b>5</b>
<b>4.0    <i>SUMMARY</i> .....</b>	<b>6</b>
<b>4.1    Points of Contact.....</b>	<b>6</b>

# **PRIVACY IMPACT ASSESSMENT**

## **Financial Management Systems**

### **1.0 PRIVACY IMPACT ASSESSMENT METHODOLOGY**

This Privacy Impact Assessment (PIA) was completed using the United States Department of Agriculture (USDA) guidelines on privacy dated 24 October 2002. Information was collected from interviews with the data owners of the system, system administrators and developers, and from internal and external audits.

#### **1.1 Background**

The USDA is responsible for ensuring the privacy, confidentiality, integrity, and availability of customer and employee information. The USDA recognizes that privacy protection is both a personal and fundamental right of its customers and employees. Among the most basic of customers and employees' rights is an expectation that USDA will protect the confidentiality of personal, financial, and employment information. Customers and employees also have the right to expect that USDA will collect, maintain, use, and disseminate identifiable personal information and data only as authorized by law and as necessary to carry out agency responsibilities.

#### **1.2 Applicable laws, regulations, policies and procedures**

The Federal Crop Insurance Act, as amended (7 USC 1501 et seq., Ch 36)

The Federal Crop Insurance Corporation (7 CFR Subtitle B, Section 4)

Privacy Act of 1974, as amended (5 USC 552a), which affords individuals the right to privacy in records that are maintained and used by Federal Agencies. Note that 5 USC 552a includes the Computer Matching and Privacy Act of 1988 (Public Law 100-503)

Computer Security Act of 1987 (Public Law 100-235), which establishes minimum security practices for Federal computer systems

OMB Circular A-130, Management of Federal Information Resources, which provides instructions to Federal agencies on how to comply with the fair information practices and security requirements for operating automated information systems

Freedom of Information Act, as amended (5 USC 552), which provides for the disclosure of information maintained by Federal agencies to the public while allowing limited protections for privacy.

#### **1.3 Systems of Records Notice**

A Systems of Records Notice contains the "rules" of which a system must follow if it houses data on individuals. Each individual system must have its own System of Records Notice. These records can be found in the Federal General Register and in the Privacy Act Issuances that are released every two years by the Government Printing Office. The Systems of Records notices that this investments falls under include:

FCIC-1: Accounts Receivable

FCIC-8: Ineligible Requests

FCIC-10: Policyholder

# **PRIVACY IMPACT ASSESSMENT**

## **Financial Management Systems**

### **2.0 ROLES AND RESPONSIBILITIES**

The agency ISSPM is responsible for completing the PIA on all systems under their control. They will work closely with the system owners and developers to correctly identify privacy risks that are generated from the system. When the PIA is completed, the ISSPM will forward the completed PIA to the Department Privacy Policy Analyst for further analysis and a determination of the need of the system. The Privacy Policy Analyst, ISSPM, and system owner will incorporate design requirements into the system to resolve privacy risks.

### **3.0 ASSESSMENT**

Information in this investment contains, but is not limited to: Social Security Numbers, Producer Names, Tax IDs for Insurance Providers, and Financial Information for Insurance Providers. Use of this data is necessary as this investment provides for the payment to/from private Insurance Providers of premium or indemnity owed to/from RMA. Systems in this investment also track ineligible claims, reconcile RMA's financial accounts, and the Plan of Operations, which contains the financial data on the Insurance Providers.

#### **3.1 Data in the system**

Data in the system primarily comes from the Policy database. This database contains every record conceivable for crop insurance, ranging from the Social Security Number (SSN) for agents and producers to the types of crops insured for a particular farm. These databases are populated using the Data Acceptance System's ISAM processes. This process takes the data received from the private Insurance Providers and files it into the correct table in the Policy and other databases. The Data Acceptance System validates this data when it arrives and checks it against the Actuarial Data Master database for the correct format, redundancy, and ineligible requests. Data for the Ineligible Tracking System does not go through DAS edits, it performs its own editing and validation of data, but input is otherwise sent through the same steps as input to the DAS system. The Debt Management System tracks information from data (e.g., Social Security Numbers) provided by the IRS and Department of the Treasury. This data allows the agency to collect monies owed by the producer from certain government payments.

The accounting cycle begins the Saturday of the first full week of any month. Data is cutoff at this time and the data is reconciled against accounting databases. At this time, the accounting databases are populated and payments can be made to the Insurance Providers. The data is required to be up-to-date by the terms of the Standard Reinsurance Agreement (SRA). The SRA provides for penalties for late submission of data by an Insurance Provider. While data input to the system comes from Insurance Providers, and is about individual producers and policies, no data is directly received, gathered, or requested from individuals.

Data is processed in the Ineligible Tracking System from insurance providers. This system tracks producers that have become ineligible to participate in the crop insurance program for any number of reasons. This data is held in the system indefinitely. This data is shared among the various insurance providers so that no single producer can defraud the system. Insurance

## **PRIVACY IMPACT ASSESSMENT**

### **Financial Management Systems**

Providers are bound by the terms in the Standard Reinsurance Agreement to keep this information confidential, and penalties may be levied against companies that do not follow the terms of the agreement.

### **3.2 Access to the data**

Access to the data is limited to the Fiscal Services Branch accountants, System Administrators, and Database Administrators. This access is determined by job function and the position that each individual is assigned. In addition, each individual's supervisor determines if the individual's job position requires access. Access is further restricted to the specific databases and tables that the individual needs to perform their duties.

The individual's Security Liaison Representative (SLR) fills out an FCIC-586 *User Request Form* that not only requests access to the general support system, but also requests access to the specific databases required for job performance. This form is routed to RMA Security where it is reviewed for approval. Once security approves the access, the form is returned to the SLR for distribution to the UNIX staff and to the proper DBA.

The RMA ISSPM and the branch SLR are responsible for ensuring that privacy is protected through the proper use of security controls. Privacy is treated the same as the basic security tenant of confidentiality when security controls are evaluated and employed on the system. In this manner, while not explicitly a section on security audits and risk assessments, privacy is included in the overall security plan of the system.

### **3.3 Attributes of the data**

The data is necessary to determine actual amounts of premium owed RMA or RMA's share of indemnity by the Insurance Providers. The data is used to reconcile claims that the Insurance Providers provide to RMA. Data is also used in the Ineligible Tracking System to compare that data with ineligible requests.

The system does not track individuals except for the Ineligible Tracking System. This does not monitor other than to keep track of ineligible requests. Insurance Providers can request additions or removals from this system at any time. The system does not have the ability to derive new data from the information in the system.

Accounting reports are produced on the Insurance Providers, but no reporting functions by individual occur on the systems covered in this investment, other than the ineligible requests that are generated on a by request basis. These requests are available to the Insurance Providers as part of the Standard Reinsurance Agreement.

### **3.4 Maintenance of Administrative controls**

This system does not take into account race, sex, national origin, or other attributes that may be used in a matter that does not meet with the requirements of the Risk Management Agency, United States Department of Agriculture, or the Constitution of the United States of America. As such, it has been designed to report only on attributes such as Social Security Number (for agent and producer) and items such as indemnity, premium owed, and crop insured, as an example.

Records are maintained for a maximum of five years, after which they are overwritten and destroyed, with the exception of the Ineligible Tracking System. Until that point, Insurance

## **PRIVACY IMPACT ASSESSMENT**

### **Financial Management Systems**

Providers may submit claims to currently active years, subject to the terms of the Standard Reinsurance Agreement. Each of the databases and tables are protected so that only authorized individuals are allowed access to that database.

#### **4.0 SUMMARY**

Privacy is an ongoing process that is becoming evermore entwined with security in Information Systems. The USDA is committed to protecting customer and employee data by addressing the following issues in regards to privacy:

1. The use of information must be controlled
2. Information may only be used for a necessary and lawful purpose.
3. Individuals must be informed in writing of the principal purpose and routine uses of the information being collected from them.
4. Information collected for a particular purpose should not be used for another purpose without the data subject's consent unless such other uses are specifically authorized or mandated by law.
5. Any information used must be sufficiently accurate, relevant, timely, and complete to assure fair treatment of the individual.

This investment does not store any individual data other than that in the Ineligible Tracking System, this system is specifically addressed in the FCIC-8 Systems of Records Notice. Other data is used for reconciliation and audit purposes but is not stored by this system or used to generate reports.

#### **4.1 Points of Contact**

Investment Owner: Denise Hoffman; Director Reinsurance Services Division  
(816) 926-3406 [denise.hoffman@rma.usda.gov](mailto:denise.hoffman@rma.usda.gov)

Investment Manager: Lonnie Clemon; Chief, Fiscal Operations Branch  
(816) 926-3038 [lonnie.clemon@rma.usda.gov](mailto:lonnie.clemon@rma.usda.gov)

IT Security Manager: Karen Grissom; Information Systems Security Manager  
(816) 926-1341 [karen.grissom@rma.usda.gov](mailto:karen.grissom@rma.usda.gov)

IT Security Officer: Eric Baer – CISSP; Information Security Officer  
(816) 823-1950 [eric.baer@rma.usda.gov](mailto:eric.baer@rma.usda.gov)